Remarks

Claims 1-63 were pending. Claim 64 is newly presented. Claims 1-64 are pending.

The Examiner rejected Claims 1-52, 55-56 and 63 under 35 U.S.C. § 103(a) as being unpatentable over the article "Fast Inter-AP Handoff using Predictive Authentication Scheme in a Public Wireless Network." ("Choi"), in view of U.S. Patent 6,876,747 ("Faccin") and in view of U.S. Patent Application 2004/0014422 ("Kallio"). With respect to Claim 1, the Examiner states:

> Cl. A method for handoff in a wireless communication network, comprising: generating a handoff encryption key [Page 1, Introduction, Lines 11-141 handing off a wireless terminal from a first access point to a second access point [Page 1, Introduction, Lines 11-141 and communicating data packets, between the second access point and the wireless terminal and authenticating the wireless terminal [Page 1, Introduction, Lines 11-14, page 6, 3.2 lines 8-15, page 7, Fig. 5, 6]. Choi teaches the re-authentication after handoff as shown in Fig. 6. Choi doesn't expressively mention communicating data packets encrypted with the handoff encryption key, between the second access point and the wireless terminal for immediate secured data transmission (i.e. secure data transmission during the handoff without perceivable interruption).
>
> Faccin teaches communicating data packets encrypted with the handoff encryption key, between the second access point and the wireless terminal for immediate secured data transmission (secure data transmission during the handoff without perceivable interruption i.e. before the authentication of the wireless terminal) [col. 2 lines 1-16, Fig. 1, 5].
>
> Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Faccin with Choi, since one would have been motivated to provide security mobility between two cellular systems [Faccin, col. 1 lines 9-10].
>
> Kallio teaches initiating authentication of the wireless terminal with an authentication server and communicating encrypted data packets between the second access point and the wireless terminal before the authentication of the wireless

terminal is completed [Fig. 13, paragraph 0148-0152, 0155-0158, Fig. 14].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Kallio with Choi and Faccin, since one would have been motivated to provide efficient transition/handover from a first access point to a second access point [Kallio, paragraph 0013, 0014].

Applicants respectfully traverse the Examiner's rejection. As the Examiner noted, Claim 1 recites a method by which secured data transmission is carried out immediately upon handoff and before authentication is complete:

1. A method for handoff in a wireless communication network, comprising:

generating a handoff encryption key;

handing off a wireless terminal from a first access point to a second access point; and

initiating authentication of the wireless terminal with an authentication server and communicating data packets encrypted with the handoff encryption key between the second access point and the wireless terminal for immediate secured data transmission before authentication of the wireless terminal is completed.

As explained in Applicants' Specification, at page 15, paragraphs [0060]-[0063], the above-underscored limitations allows data transmission during the handoff without perceivable interruption due to the latency of authentication with an authentication server.

Contrary to the Examiner's assertion quoted above, Kallio does not teach "initiating authentication of the wireless terminal with an authentication server and communicating encrypted data packets between the second access point and the wireless terminal before the authentication of the wireless terminal is completed." In fact, Kallio's Figs. 13 and 14 – on which the Examiner bases his rejection – show that authentication between the terminal device and the authentication server (step 1322) completes before secured data transmission

(i.e., encrypted data transmission) is carried out between the terminal device and access point 2 at step 1322. In addition, Kallio expressly states that data transmission occurs after authentication:

> [0164] A step 1332 follows step 1330. In this step, the link (e.g., a Bluetooth link) between access point 406 and terminal device 402 is authenticated based on the link key (i.e., group key) accessed in step 1328. Therefore, this authentication process does not require pairing to be performed. After authentication, steps 1334 is performed. In this step, an encryption key for secure communications is established between terminal device 402 and access point 406.
>
> [0165] FIG. 14 shows a sequence of steps involving techniques of the present invention where terminal device 402 establishes a link with access point 406 in a manner that is different from FIG. 13. In particular, FIG. 14 replaces steps 1306, 1308, and 1310 with a step 1402.
>
> (emphasis added; Kallio, at page 3, paragraphs [0164-0165]

Applicants therefore respecfully submit that the Examiner is mistaken regarding Kallio's teachings. Thus, the combined teachings of Choi, Faccin and Kallio do not meet the limitations of amended Claim 1. Accordingly, Claim 1 and its dependent Claims 2-27 are each allowable over the combined teachings of Choi, Faccin and Kallio. Similarly, independent Claims 28, 34, 41, 49, 55-56, and 63 -- which each also recite secured data transmission using a handoff encryption key occurs while an authentication process is being carried out and before completion of the authentication -- and their respective dependent Claims 29-33, 35-40, 41-48, 50-52, are each allowable over the cobmined teachings of Choi, Faccin and Kallio. Reconsideration and allowance of Claims 1-52, 55-56 and 63 are therefore requested.

The Examiner rejected Claims 53-54 and 57-62 under 35 U.S.C. § 103(a) as being unpatentable over Choi, in view of Faccin. With respect to independent Claims 53 and 57, the

Examiner states:

> A wireless access point comprising a memory which stores: instructions to receive a handoff encryption key generation secret parameter from an authentication server; instructions to receive a first packet from a wireless terminal, wherein the first packet includes an address of the wireless terminal; instructions to generate a handoff encryption key as a function of the handoff encryption key generation secret parameter and the address of the wireless terminal; and instructions to transmit the handoff encryption key to a wireless terminal [Page 1, Introduction, Lines 11-14 *and* Page 7, §3.2, Lines 4-15., Transposing functionality from one logical unit to another to forgo network communication is well known in the art and deemed obvious, and key generation by parameters (MAC, IP address, etcetera) is outlined within the taught use of IAPP (Page 2, Lines 11-15). Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification].
>
> * * *
>
> A handoff encryption key generator in a wireless communication network, comprising: an input to receive a handoff encryption key generation secret parameter; an input to receive an open parameter; and a generator for generating a handoff encryption key as a function of the handoff encryption key generation secret parameter and the open parameter [Page 1, Introduction, Lines 11-14, 6-11, 17-19 *and* Page 7, §3.2, Lines 4-15, Fig. 5, 6].

Applicants respectfully traverse the Examiner's rejection. First, Applicants are puzzled by the Examiner's statement regarding Claim 53 that "transposing functionality from one logical unit to another to forgo network communication is well known in the art and deemed obvious." Nothing in Applicants' Claim 53 relates to "transposing functionality from one logical unit to another to forgo network communication." Therefore, Applicants request that the Examiner provide a more detailed explanation as to which limitations of Applicants' Cliam 53 was the Examiner referring. Further, Claims 53 and 57 recite generating an encryption key based on at least a handoff encryption key generation secret parameter and the address of the wireless terminal or an open parameter:

53. (Previously presented) A computer readable medium storing computer-executable instructions for execution by a central processing unit in a wireless access point comprising:

instructions to receive a handoff encryption key generation secret parameter from an authentication server;

instructions to receive a first packet from a wireless terminal, wherein the first packet includes an address of the wireless terminal;

instructions to generate a handoff encryption key as a function of the handoff encryption key generation secret parameter and the address of the wireless terminal; and

instructions to transmit the handoff encryption key to a wireless terminal.

* * *

57. A method for generating a handoff encryption key generator in a wireless communication network, comprising:

Receiving a handoff encryption key generation secret parameter;

receiving an open parameter; and

generating a handoff encryption key as a function of the handoff encryption key generation secret parameter and the open parameter.

(emphasis added)

Applicants' are unable to locate any teachings in the portions of Choi that the Examiner cited (i.e., page 1, lines 6-14, 17-19, page 2, lines 11-15, Figs. 5-6, or page 7, lines 4-15) that relate to handoff encryption key generation parameters. Choi merely teaches, at page 1, that "a mobile host (MH) ... should perform a new user authentication procedure and receive a new Wired Equivalent Privacy (WEP) key, ..." The article "IAPP Enhancement Protocol" ("Jin") also neither discloses nor suggests such handoff encryption key generation

parameters. The Examiner's further guidance as to how Choi's or Jin's teachings map into the limitations of Claims 53 and 57 is therefore requested. In contrast, Claims 53-54 and 57-62 each recite a specific algorithm for generating a handoff encryption key – i.e., using "an address of the wireless terminal" or "an open parameter" with a "secret parameter." Such an algorithm is neither disclosed nor suggested by Choi, Faccin or Jin. Accordingly, Claims 53-54 and 57-62 are also each allowable over the combined teachings of Choi, Faccin and Jin, individually and in any combination. Accordingly, reconsideration and allowance of Claims 53-54 and 57-62 are requested.

The Examiner provisionally rejected Claims 1-63 under the doctrine of non-statutory obviousness-type double patenting over Claims 1-25 of U.S. patent application, serial no. 10/290,650. However, as allowable subject matter has been indicated in neither this application nor the copending '650 application. Accordingly, the Examiner's rejection of Claims 1-63 is premature. Applicants will address substantively the Examiner's double-patenting rejection when the Examiner indicates allowable subject matter in this application when the Examiner indicates that the claims in this application or the copending application are allowable.

Newly presented Claim 64 is believed to be allowable over the prior art of record.

Therefore, for the reasons set forth above, all pending claims (i.e., Claims 1-64) are allowable over the art of record. If the Examiner has any question regarding the above, the Examiner is respectfully requested to telephone the undersigned Attorney for Applicant at 408-392-9250.

Certificate of Transmission: I hereby certify that this correspondence is being transmitted to the United States Patent and Trademark Office (USPTO) via the USPTO's electronic filing system on December 19, 2008.

Attorney for Applicant(s) — Date of Signature: 12/19/2008

Respectfully submitted,

Edward C. Kwok
Attorney for Applicant(s)
Reg. No. 33,938

Law Offices of
MacPherson Kwok Chen & Heid LLP
2033 Gateway Place, Suite 400
San Jose, CA 95110
Tel: (408) 392-9250
Fax: (408) 392-9262